

REMARKS

This communication is in response to the Office Action mailed December 23, 2003 in connection with the above-identified matter. Claims 14, 15, 18, 19, 20 and 22 have been amended to correct for grammatical errors and so that the claims conform with customary U.S. patent drafting rules, not to overcome prior art rejections. Claims 23-26 have been added. No new matter has been added. Claims 14-26 remain pending in this application with claims 14 and 19 being the only independent claims. Reconsideration of the outstanding rejections in view of the amendments to the claims and remarks presented below is respectfully requested.

In the outstanding Office Action, claims 14-22 are rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 5,793,866 (Brown et al.).

The present invention is directed to a method and apparatus for personalization of a GSM chip card when the subscriber first logs on to the mobile radio network. In accordance with the invention, the device manufacturer/chip manufacturer applies initial (pre-personalization) data associated with the card to the chip. Pre-personalization at the chip manufacturer is carried out by allocating a range of card numbers (ICCID) and subscriber identification (IMSI). The chip itself derives from a secret key K1 which is known to the chip manufacturer an initial secret key Ki_1, while PIN and PUK may be set to default values. The network operator performs the actual personalization at a later time and only for those customers who enter into a contract with the network operator.

Independent claims 14 and 19 are distinguishable over Brown. A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). In general the present invention is distinguishable over Brown in that it is directed to personalization of a GSM chip card, whereas the prior art reference relates to an authentication procedure for a remote communication device.

Reply to Office Action of December 23, 2003
U.S. Serial No. 09/485,352

Page 5

Despite the fact that the remote communication device may include a GSM chip or card, the patented invention is not directed towards personalization of the GSM chip or card that may be employed in the remote device, but instead to authentication of the remote device itself.

Because of this distinction in overall functionality the claims of the present invention differ structurally over that disclosed or suggested by Brown. For example, since the present invention is directed towards personalization of the GSM chip, claims 14 and 19 call for storing in the chip "a subscriber identification number (IMSI)" and "a card number (ICCID)" associated with the GSM chip. In contrast, Brown relates to authentication of a remote device and discloses storing in the remote device "a telephone number and subscription ID" (emphasis added)(Col. 4, ll. 17-19). Brown fails to teach storage of the card number, as found in claims 14 and 19, because there is no discussion of personalization of the GSM card, only authentication of a remote device for which storage of its telephone number is sufficient.

Furthermore, claims 14 and 19 call for storing of the subscriber identification number (IMSI) and the card number (ICCID) to take place "at the manufacturer" as part of the process of "pre-personalizing the chip". Brown, on the other hand, discloses (Col. 4, ll. 39-52) that the subscription identification is not initially provided by the manufacturer.

"The service provider, a central site, can also include a home location register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning. It has become desirable for over-the-air service provisioning to provide the subscription ID to the remote device 104, a mobile subscriber in the cellular system. This allows the subscription ID to be down-loaded from the central site 102, the service provider facility, to the subscriber remote device 104. In the OTASP protocol, a subscriber purchases a "blank" remote device, which is a remote device having no subscription ID. This remote device can originate a special purpose call to any of several service providers (such as service provider central site 102) to request activation." (emphasis added)

Unlike claims 14 and 19 which expressly call for the subscriber identification number (IMSI) and the card number (ICCID) to take place "at the manufacturer" as part of the process of "pre-personalizing the chip", Brown discloses that the subscription ID is not part of the remote device when purchased by the subscriber.

Reply to Office Action of December 23, 2003
U.S. Serial No. 09/485,352

Page 6

Step b) of claim 14 is further distinguishable over the prior art in that it calls for the chip itself to derive "an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip" at the manufacturer (as stated in the preamble of claim 14). Accordingly, the manufacturer provides the secret key Ki stored at the chip. From this stored secret key Ki , the initial secret key Ki_1 is derived by the chip. In contrast, Brown discloses that "the public-key modulus $N1$ is transmitted to the remote device 104 from the service provider controller 108. $N1$ is the public modulus, and it is the product of $P1$ and $Q1$, two secret numbers stored in the memory 114 (which is specified in Col. 4, l. 38 as being at the service provider central site 102 facility) and having a known criteria. The remote device 104 responds to the modulus $N1$ by generating a ciphertext number C , which is a function of the modulus $N1$, a random number n generated by the remote device 104, and an arbitrary number e . The value of e is known to both the remote device 104 and the central site 102." In contrast to claim 14, in which the manufacturer provides the secret key Ki and thereafter, the chip itself derives the initial secret key Ki_1 therefrom, Brown discloses that the public-key modulus $N1$ (analogous to the secret key Ki) is provided to the remote device 104 from the service provider controller 108, not the chip manufacturer.

Furthermore, step b) of claim 14 also calls for PIN (Personal Identification Number) and PUK (Personal Unblocking Key) to be set to a default value. These terms are terms of art in the mobile telephony industry and have specific conventional definitions. The Examiner in the outstanding Office Action states that Col. 4, l. 63 of Brown teaches this limitation. The relevant passage reads " $N1$ is the public modulus, and it is the product of $P1$ and $Q1$, two secret numbers stored in the memory 114 and having a known criteria." Brown fails to disclose that $P1$ and $Q1$ correspond to the PIN and the PUK, respectively. To the contrary, Brown discloses these two numbers as being relevant to deriving the public modulus $N1$. In addition, clearly Brown fails to disclose or suggest setting $P1$ and $Q1$ to default values.

With respect to step c) of claim 14, despite Brown generically disclosing (Col. 4, ll. 39-40) that the central site can include a home location register and an authentication center, the reference fails to expressly disclose making an entry in an authentication center (AC) and a home

location register (HLR) as soon as the subscriber has entered into a contract with a network operator, as found in claim 14.

Yet another distinguishing feature of the present invention is found in step d) of claim 14 which calls for "deriving at the authentication center (AC) the initial secret key Ki_1 " from the secret key Ki (as expressed in step b)). Brown, on the other hand, teaches (Col. 5, ll. 2-4) that "When the ciphertext number C is received by the service provider, it is decoded using the equation $n = C^{d1} \bmod N1$, to determine n . The random number n is subsequently used to encrypt the authentication key, otherwise known as the A-key." Based on the Examiner's statements, if C is analogous to the claimed initial secret key Ki_1 , then the number n from which it was derived must be analogous to the claimed secret key Ki . This is not the case, since the patent expressly discloses in the passage quoted above that the number n is a random number, not a secret key Ki .

Claim 14 is still further distinguishable over the art of record in that step g) calls for "negotiating between the chip and the security center (SC) a new second secret key Ki_2 ". The Examiner maintains that this limitation is taught by Brown (Col. 5, ll. 4-8) The random number n is subsequently used to encrypt the authentication key, otherwise known as the A-key. The encrypted A-key is communicated to the remote device 104 from the service provider central site 102." The authentication key (A-key) is not a new second secret key Ki_2 negotiated between the chip and security center, but instead is encrypted at the service provider 102 and then communicated to the remote device 104. Independent claim 19 contains a similar limitation and thus is patentable over Brown for at least the same reasons expressed above with respect to claim 14.

Step h) of claim 14 calls for disabling the conditions of step e), i.e., disabling the conditions of the network to automatically connect the chip to the security center. Under such circumstances, the procedure for forced personalization of the chip is now completed and disabled so that the subscriber can make regular use of the chip card (mobile phone). This has nothing to do with aborting the personalization process, but instead is merely the completion of the personalization procedure. The Examiner relies on Brown for the teaching (Col. 6, ll. 19-23) that "If the numbers do not match, the OTASP process is aborted. This provides security since it


will be difficult for the intruder to continue operating between remote device 104 and central site 102 and to mimic the voice of the subscriber without introducing a substantial delay period." Once again, this is not analogous to the claimed step in which conditions are disabled not to abort the personalization process, but because the process has been completed and finished.

Dependent claim 17 is further distinguishable over the art of record in that it states that "the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag)". The Examiner in rejecting the claim refers to Col. 6, ll. 15-23 that reads "The controller 108 of the central site 102 likewise generates a number for display 118 having the same relationship to the modulus N1. The user can then read the characters on the display 148 to the service provider operator, who is simultaneously reading the display 118. If the numbers do not match, the OTASP process is aborted. This provides security since it will be difficult for the intruder to continue operating between remote device 104 and central site 102 and to mimic the voice of the subscriber without introducing a substantial delay period." This passage cited by the Examiner fails to disclose or suggest setting and deleting a rerouting command (hotlining flag) in the HLR so that during logon to the network, a connection is established from the chip to the security center. The Examiner has failed to establish why the implementation of a different security feature disclosed in Brown is analogous to the feature expressly stated in claim 17.

For the foregoing reasons applicant submits that independent claims 14 and 19 are patentable over the prior art of record. The remaining claims depend from one of these independent claims and thus are also patentable over the art of record. Applicants submit that the application is in condition for allowance and passage to issuance is respectfully requested.

If any additional fees are required, authorization is hereby provided to charge our U.S. Patent and Trademark Deposit Account No. 14-1263.

Respectfully submitted,


Christa Hildebrand
Reg. No. 34,953
Attorney for Applicant

Norris McLaughlin & Marcus P.C.
220 East 42nd Street, 30th Floor
New York, N.Y. 10017
Telephone: (212)808-0700
Facsimile: (212)808-0844

Reply to Office Action of December 23, 2003
U.S. Serial No. 09/485,352

Page 10